



SureServer/SureServer EV

Microsoft IIS8.0/8.5

CSR 作成/証明書インストール手順書

(新規・更新用)

Version 1.5

PUBLIC RELEASE

2017/06/01

改訂履歴

日付	バージョン	内容
2014/02/10	1.0	初版リリース
2015/02/09	1.1	クロスルート証明書の変更に伴う修正
2016/09/01	1.2	「IIS8.5」の記述を追加
2016/12/15	1.3	「はじめに」の記述内容を修正
2017/04/28	1.4	「OU」に関する記述内容を修正
2017/06/01	1.5	「O」と「OU」およびクロスルート設定時の注意事項を追記

目次

はじめに.....	4
サーバ証明書お申込みフロー	5
CSR の作成.....	6
1. CSR 作成前のご確認事項.....	7
1.1. 公開鍵長のご指定について.....	7
1.2. CSR 作成時に指定する項目 (DN)について.....	7
2. キーペア・CSR の作成.....	8
2.1. 作成方法	8
3. 証明書のお申し込み.....	13
証明書のインストール	14
4. 証明書のダウンロード	15
4.1. 中間 CA 証明書のダウンロード.....	15
4.2. SSL サーバ証明書のダウンロード.....	15
5. 証明書のインストール.....	16
5.1. 中間 CA 証明書のインストール.....	16
5.2. SSL サーバ証明書のインストール.....	24
6. SSL サーバ証明書の適用	26
7. 鍵ペアファイルのバックアップ.....	29
SSL 通信の確認.....	31
8. SSL 通信の確認.....	32

はじめに

【！】本手順書をご利用の前に必ずお読みください

本ドキュメントは、Microsoft 社の「Internet Information Services 8.0/8.5(以下、IIS8.0/8.5)」の環境下でサイバートラストのサーバ証明書をご利用いただく際の CSR 作成とサーバ証明書のインストールについて解説するドキュメントです。

実際の手順はお客様の環境により異なる場合があります、IIS8.0/8.5 の動作を保証するものではありません。あらかじめご了承ください。

なお、このドキュメントは予告なく変更される場合があります、サイバートラスト株式会社はその内容に対して責任を負うものではありません。

また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。

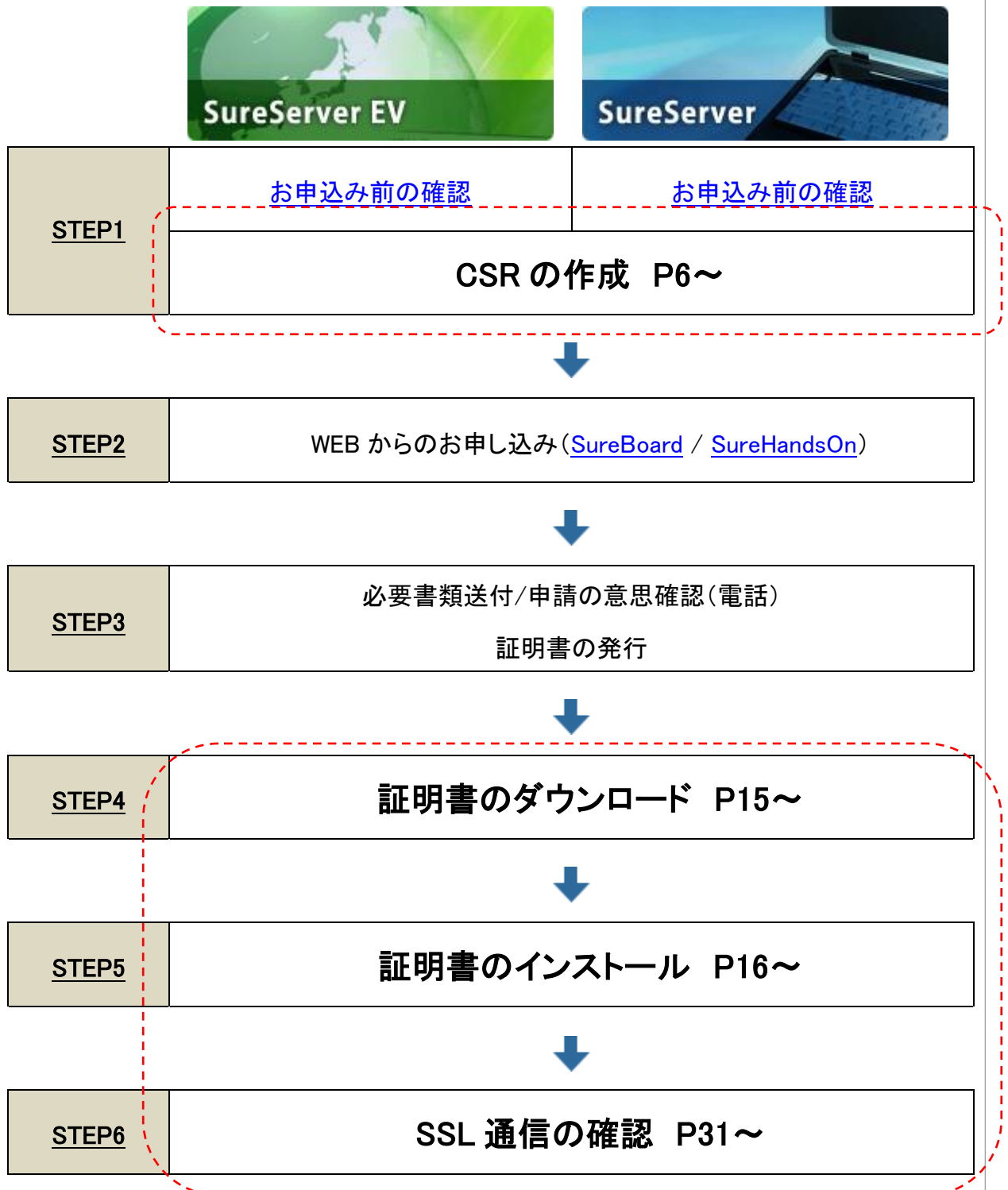
このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。

ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。

サーバ証明書お申込みフロー

サーバ証明書のご購入については、以下のお申込みフローをご確認ください。

本手順では、**赤枠**で囲まれた部分のフローをご案内しています。



CSR の作成

1. CSR 作成前のご確認事項

CSR 作成前に以下についてご確認ください。

1.1. 公開鍵長のご指定について

公開鍵長は「**2048bit**」をご指定ください。

※クラウド商品(for クラウド)、マルチドメイン商品(SureServer MD など)を含みます。

1.2. CSR 作成時に指定する項目(DN)について

詳細は以下をご確認ください。

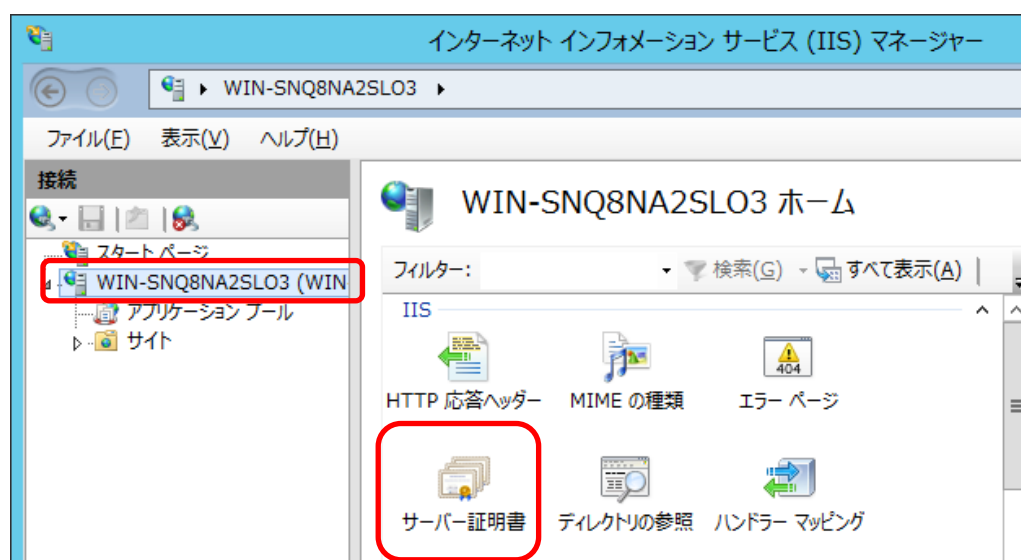
≫ [CSR 作成時に指定する項目について](#)

2. キーペア・CSR の作成

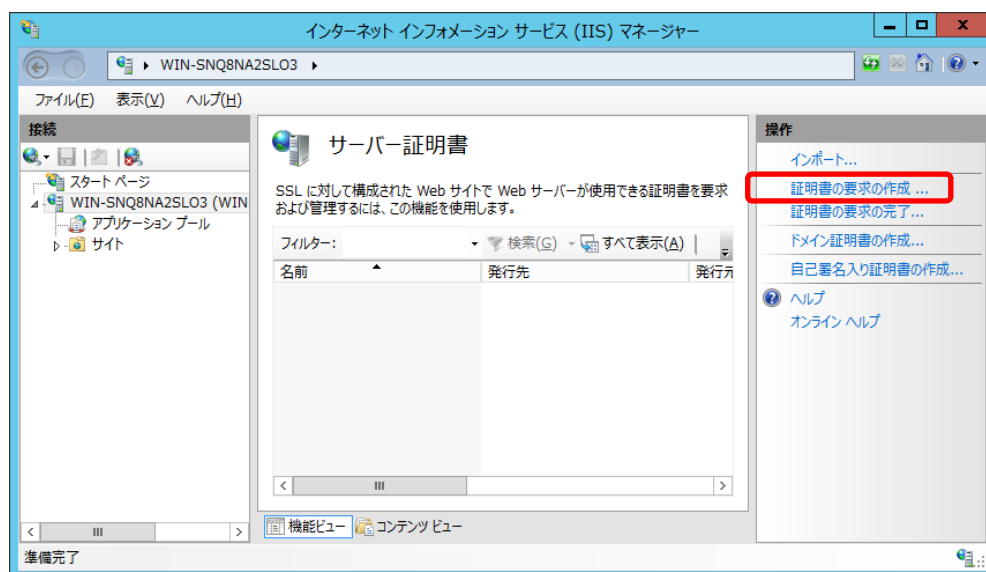
Microsoft Windows Server 2012 の【インターネット インフォメーション サービス (IIS) マネージャー】を使って、SSL で使用するキーペア(公開鍵・秘密鍵のペア)と CSR を作成します。

2.1. 作成方法

- A) 【スタート】メニューから【インターネット インフォメーション サービス (IIS) マネージャー】を選択して起動します。
- B) 以下の画面から、【サーバー証明書】をダブルクリックします。



- C) 画面右側の操作メニューから【証明書の要求の作成】をクリックします。



- D) 識別名プロパティを入力する画面が表示されますので、CSR に設定する情報を入力して、【次へ】をクリックします。以下のルールに従って正確に入力してください。

※半角英数字で入力してください。

※使用可能文字: スペース「a-z」「A-Z」「0-9」「'」「,」「()」「:」「-」「?」「&」

入力項目	内容	入力例
一般名	完全なドメイン名 (FQDN)	test.cybertrust.ne.jp
組織	申請組織の名称((英語)	Cybertrust Japan Co.,Ltd.
組織単位	「部署名」(※)	Test Unit
市区町村	申請組織の事業所住所の 「市町村名」(英語) ※東京は 23 区	Minato-ku
都道府県	申請組織の事業所住所の 「都道府県名」(英語)	Tokyo
国/地域	申請組織の国名	JP

※指定可能な値については、「[組織単位名\(OU\)について](#)」をご覧ください。

証明書の要求

識別名プロパティ

証明書に必要な情報を指定します。都道府県および市区町村に関する情報は、公式名称を指定してください。省略形は使用しないでください。

一般名(M): test.cybertrust.ne.jp
 組織(O): Cybertrust Japan Co.,Ltd.
 組織単位 (OU)(U): Test Unit
 市区町村(L): Minato-ku
 都道府県(S): Tokyo
 国/地域(R): JP

前に戻る(P) **次へ(N)** 終了(E) キャンセル

※「組織 (O)」と「組織単位 (OU)」の表示順は、IIS の入力画面と以下で異なります。CSR 作成時ならびにご確認の際はご注意ください。

発行される証明書	SSL サーバ証明書 導入サポートツール														
CN = www.cybertrust.ne.jp OU = For Test Purpose Only O = Cybertrust Japan Co.,Ltd. L = Minato-ku S = Tokyo C = JP	<table border="1"> <thead> <tr> <th colspan="2">項目</th> </tr> </thead> <tbody> <tr> <td>共通ネーム</td> <td>(CN)</td> </tr> <tr> <td>組織単位名</td> <td>(OU)</td> </tr> <tr> <td>組織名</td> <td>(O)</td> </tr> <tr> <td>市町村名</td> <td>(L)</td> </tr> <tr> <td>都道府県名</td> <td>(S/ST)</td> </tr> <tr> <td>国名</td> <td>(C)</td> </tr> </tbody> </table>	項目		共通ネーム	(CN)	組織単位名	(OU)	組織名	(O)	市町村名	(L)	都道府県名	(S/ST)	国名	(C)
項目															
共通ネーム	(CN)														
組織単位名	(OU)														
組織名	(O)														
市町村名	(L)														
都道府県名	(S/ST)														
国名	(C)														

申請サイト (SureBoard / SureHandsOn)

項目	CSR の申請内容
共通ネーム (CN)	
wwwオプション※	
組織単位名 (OU)	
組織名 (O)	
市町村名 (L)	
都道府県名 (S)	
国名 (C)	
鍵長	

E) 【暗号化サービス プロバイダー】は、表示された情報(Microsoft RSA SChannel Cryptographic Provider)を選択し、「ビット長」は「2048」と指定してください。

証明書の要求

暗号化サービス プロバイダーのプロパティ

暗号化サービス プロバイダーおよびビット長を指定します。暗号化キーのビット長は、証明書の暗号化の強度を決定します。ビット長が大きいほどセキュリティは高くなりますが、パフォーマンスが低下する可能性があります。

暗号化サービス プロバイダー(S):

Microsoft RSA SChannel Cryptographic Provider

ビット長(B):

2048

前に戻る(B) 次へ(N) 終了(E) キャンセル

F) CSR のファイル名と保存先を指定し、【終了】をクリックします。

証明書の要求

ファイル名

証明書の要求のファイル名を指定してください。この情報は署名のために証明機関に送信される可能性があります。

証明書の要求ファイル名を指定してください(P):

C:\test_csr.txt

前に戻る(P) 次へ(N) 終了(E) キャンセル

以上で、CSR の作成は完了です。

3. 証明書のお申し込み

作成した CSR をテキストエディタで開いて内容をコピーし、WEB の申請サイト ([SureBoard](#) / [SureHandsOn](#)) の申請フォームへ貼り付けて、弊社へお申し込みください。

<CSR サンプル> ※申請にはご利用いただけません。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
.
.
.
MIIEhDCCA2wCAQAwYkxGzAJBgNVBAYTAkpQMg4wDAYDVQQIDAVUub2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDA1UZXR0IFVuaXQxHjAcBgNVBAMMFXRlc3Q0Y3IiZXJ0cnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4R0cFsgRk05FgeUCaeDFyIIEST
.
.
.
-----END NEW CERTIFICATE REQUEST-----
```

「-----BEGIN NEW CERTIFICATE REQUEST-----」から、「-----END NEW CERTIFICATE REQUEST-----」までをハイフンを含め、すべてコピーし申請画面に貼り付けてください。

1文字でも欠けるとフォーマットエラーとなりますのでご注意ください。

【！】CSR 作成後の注意事項

IIS8.0/8.5 では、CSR 作成後にキーペアのバックアップを取ることができない仕様となっております。そのため、SSL サーバ証明書のインストールが完了するまでは、証明書の登録要求を絶対に削除しないでください。

※証明書の登録要求を削除されますと、元の CSR で発行した SSL サーバ証明書のインストールができなくなり、サイバートラストへの再申請が必要になります。あらかじめ、ご注意ください。

証明書のインストール

【！】本手順はサーバ証明書の発行後に行います。

4. 証明書のダウンロード

インストールが必要となる中間 CA 証明書・SSL サーバ証明書を事前にダウンロードします。

4.1. 中間 CA 証明書のダウンロード

サーバ証明書をご利用の際、お使いの機器へ中間 CA 証明書のインストールが必要となります。

ご選択いただいた商品により必要な証明書が異なりますので、証明書の種類をご確認のうえ、以下弊社ホームページからダウンロードしてください。

≫ [ルート・中間 CA 証明書のダウンロード](#)

また、ご利用商品や必要な証明書の種類がご不明の場合は、以下をご覧ください。

≫ [どの中間 CA 証明書をダウンロードすればよいですか？](#)

4.2. SSL サーバ証明書のダウンロード

SSL サーバ証明書が発行されましたら、証明書発行のお知らせのメール内リンクより事前にダウンロードし、【.cer】や【.txt】などの拡張子で保存してください。

≫ [SSL サーバ証明書のダウンロードについて](#)

5. 証明書のインストール

中間 CA 証明書と SSL サーバ証明書のインストールを行います。

5.1. 中間 CA 証明書のインストール

中間 CA 証明書を「Microsoft 管理コンソール (Microsoft Management Console: MMC)」からインストールします。

※証明書更新時、すでに同じ内容の中間 CA 証明書がインストールされている場合は、この手順をスキップしてください。

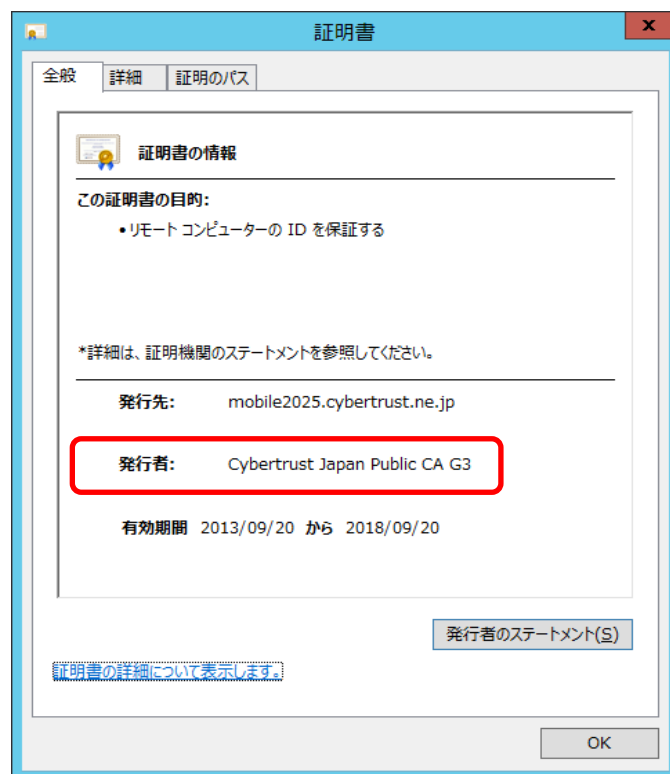
※SureServer EV[2048bit]・SureServer EV[SHA-2]、および、SureServer[2048bit]用クロスルート方式では、同様の手順で「クロスルート用中間 CA 証明書」と「中間 CA 証明書」をインストールしてください。

※クロスルート設定が正しく反映されない場合は、以下の FAQ をご確認ください。

≫ [\[IIS\] クロスルート設定が正しく反映されません。](#)

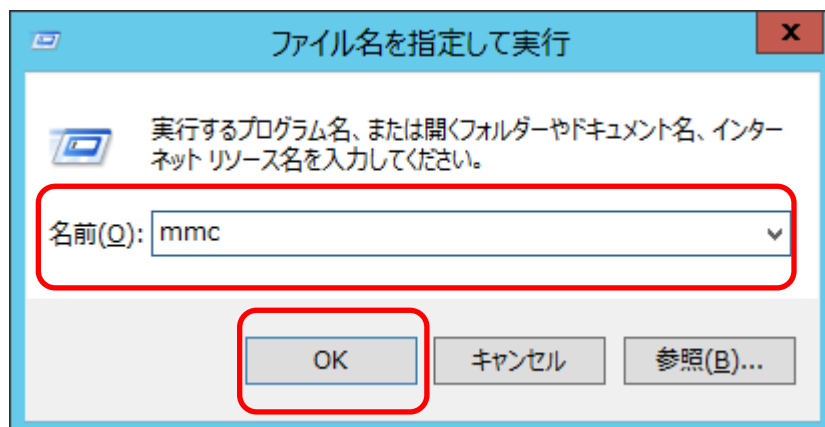
なお、必要な中間 CA 証明書のコモンネームが不明な場合は、サーバ証明書ファイルを開いて発行者のコモンネームの項目をご確認ください。

【例】SureServer[2048bit]の場合

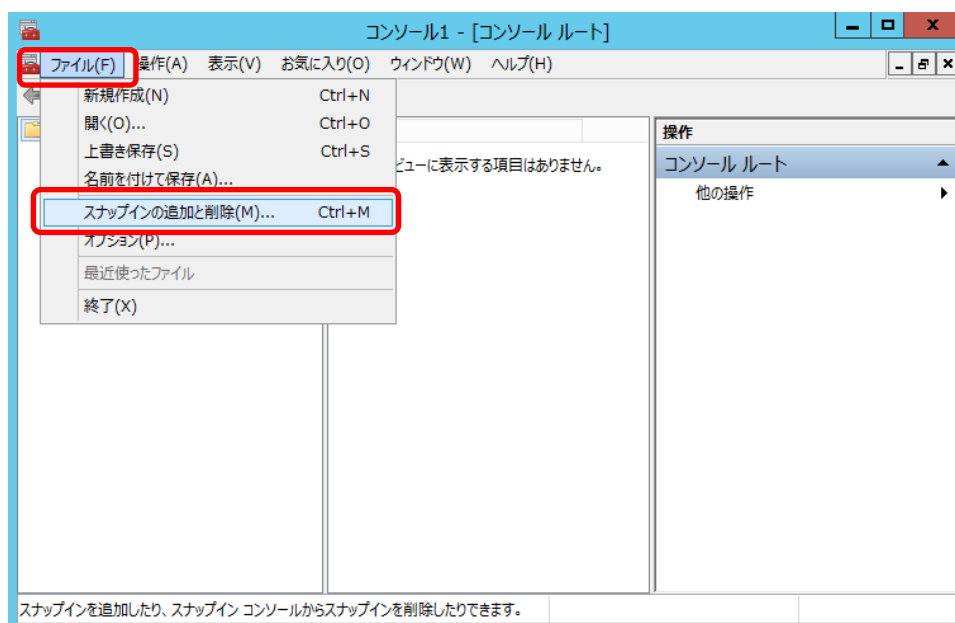


→必要な中間 CA 証明書のコモンネーム: Cybertrust Japan Public CA G3

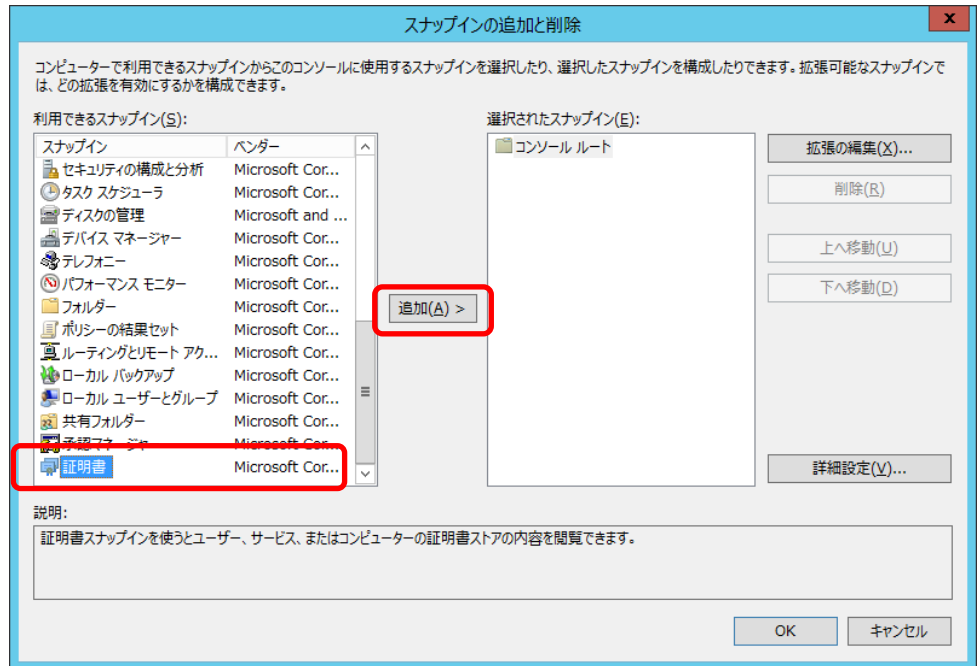
- A) 【Windows ロゴ+R キー】から【ファイル名を指定して実行】を開きます。
【名前】に「mmc」と入力して【OK】をクリックします。



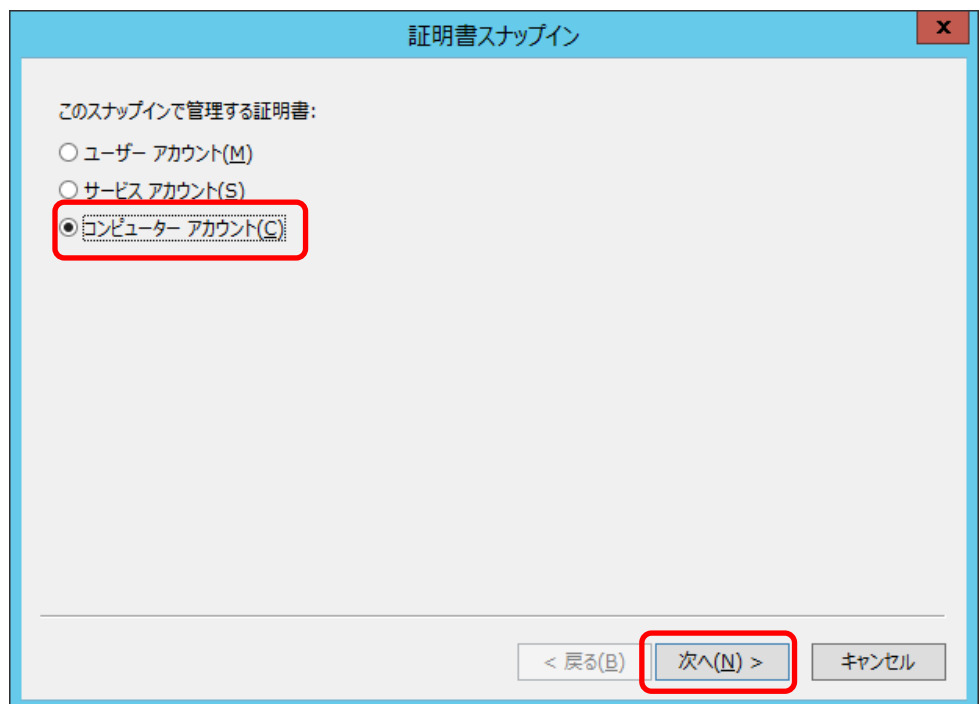
- B) MMC 画面左上の【ファイル】メニューをクリックし、【スナップインの追加と削除】をクリックします。



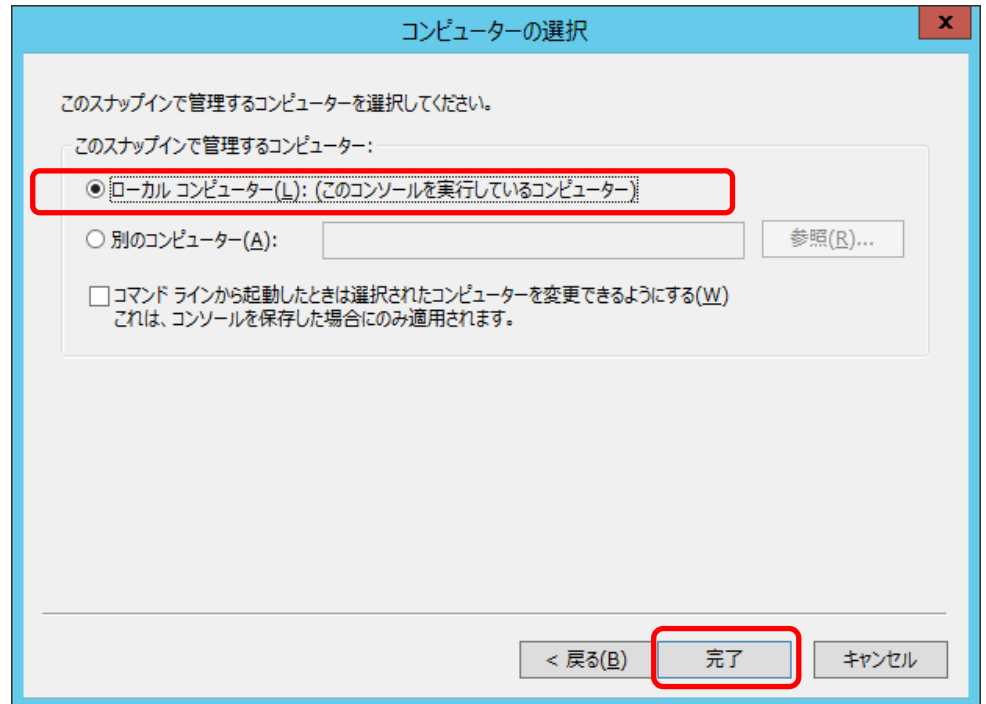
C) 【利用できるスナップイン】から【証明書】を選択し、【追加】をクリックします。



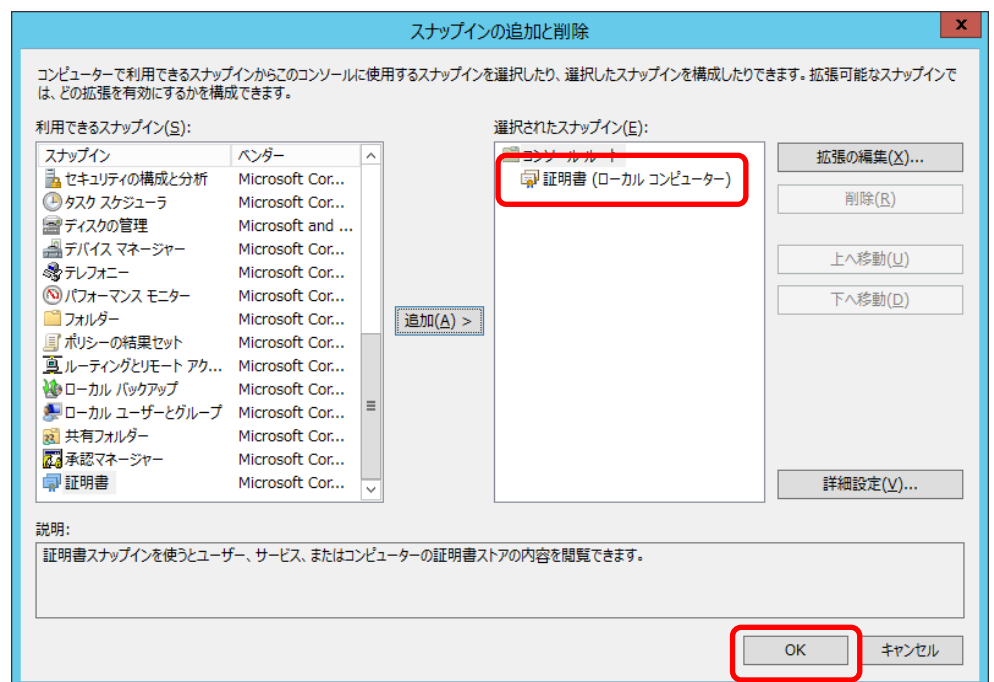
D) 【コンピューターアカウント】を選択し、【次へ】をクリックします。



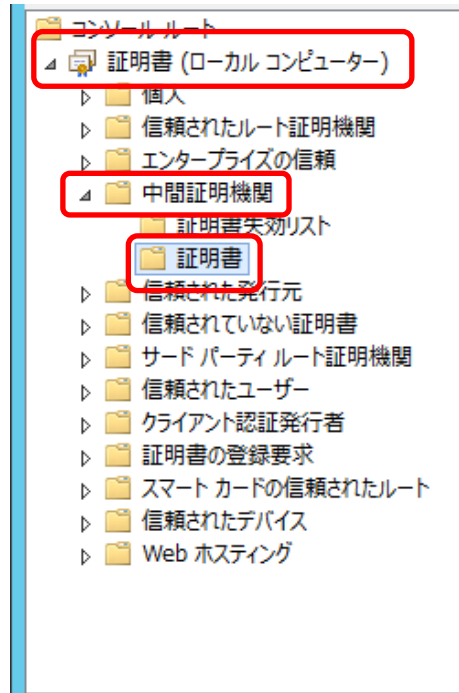
- E) 【ローカルコンピューター(このコンソールを実行しているコンピューター)】を選択し、【完了】をクリックします。



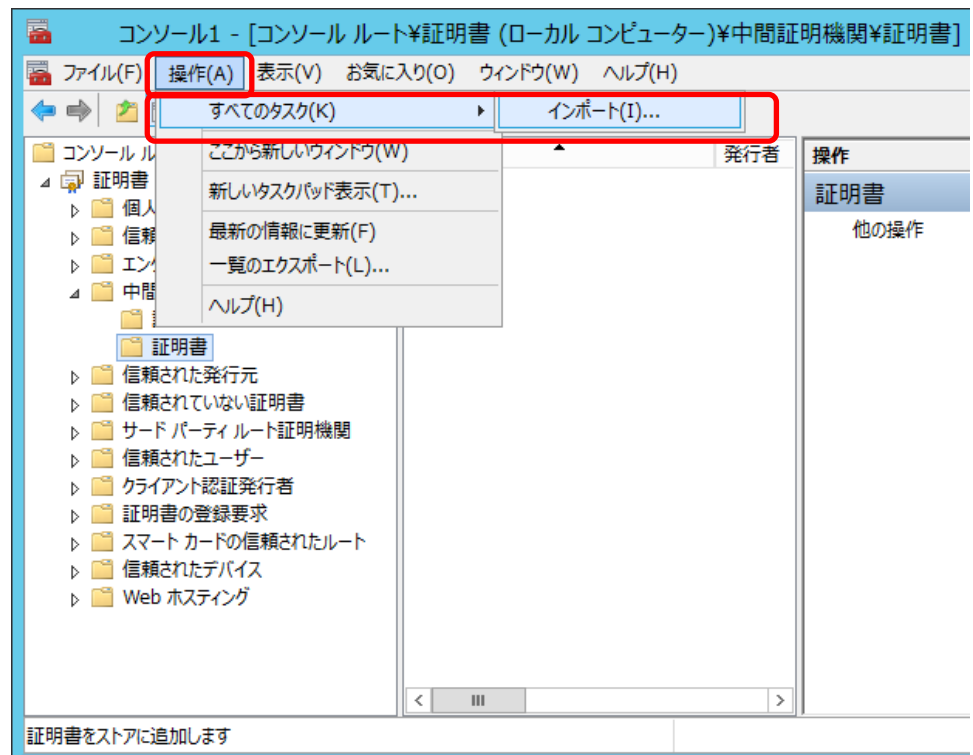
- F) 【選択されたスナップイン】に【証明書(ローカルコンピューター)】が追加されていることを確認し、【OK】をクリックします。



- G) コンソールルートへ【証明書(ローカルコンピューター)】が追加されたことを確認し、【証明書(ローカルコンピューター)】→【中間証明機関】→【証明書】をクリックします。



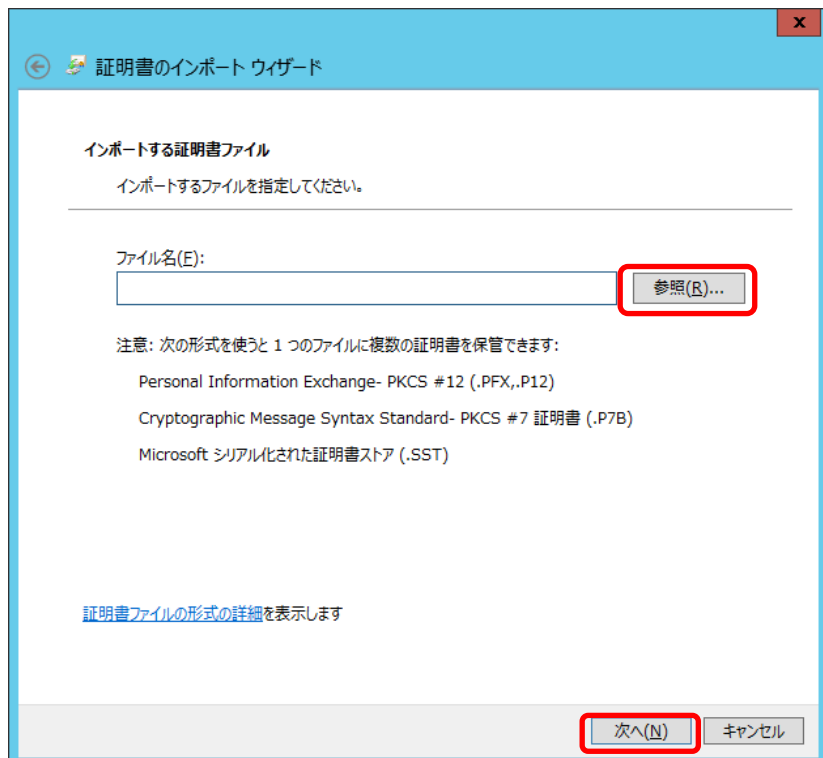
- H) MMC 画面の左上の【操作】メニュー→【すべてのタスク】→【インポート】の順にクリックします。



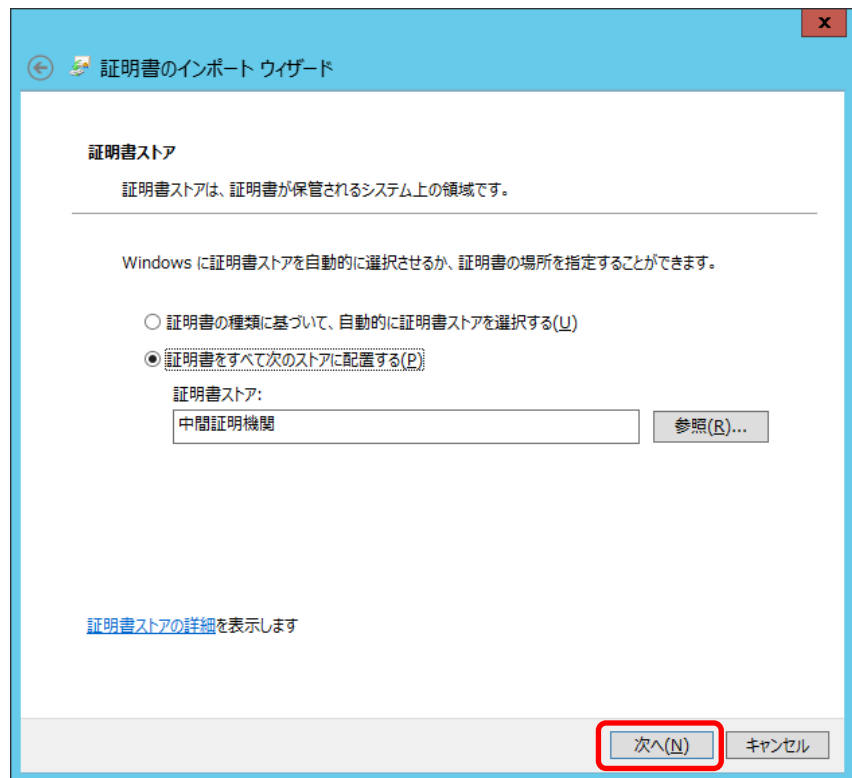
I) 証明書のインポートウィザードが表示されますので、【次へ】をクリックします。



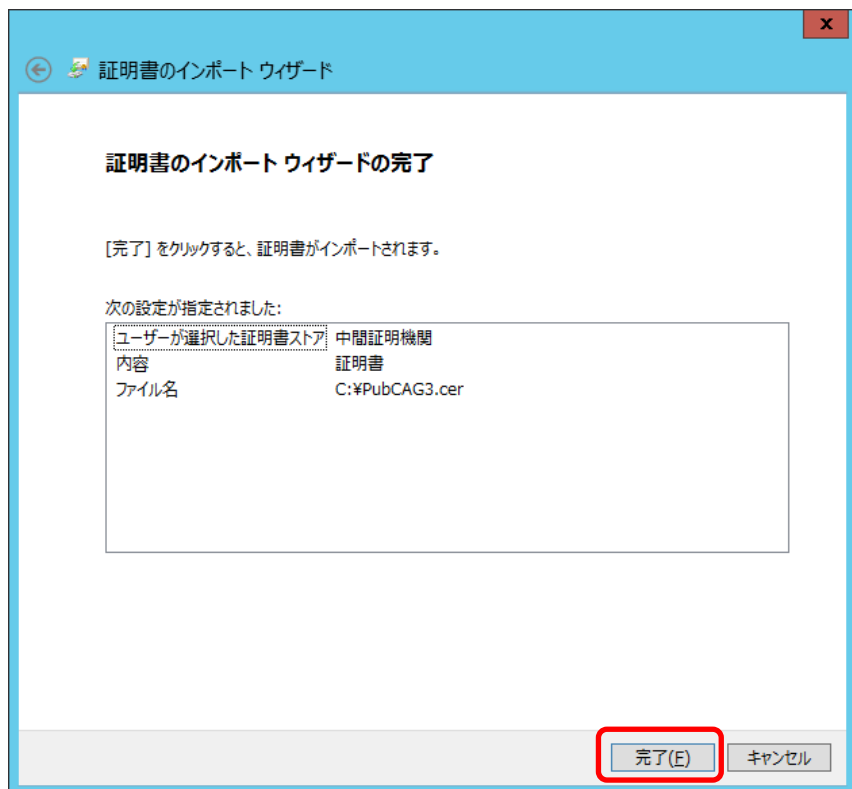
J) 【参照】をクリックしてインストールする中間 CA 証明書を指定し、【次へ】をクリックします。



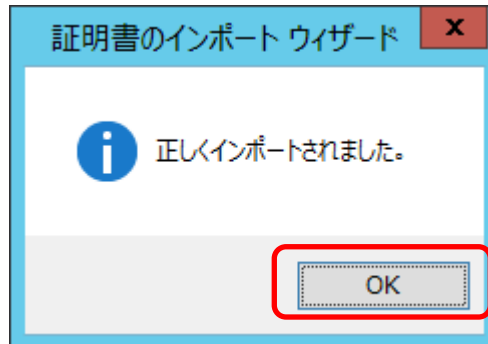
K) 【次へ】をクリックします。



L) 次の画面が表示されたら内容を確認して、【完了】をクリックします。



M) インポート正常終了のメッセージが表示されますので、【OK】をクリックします。



N) 証明書の一覧にインストールした中間 CA 証明書が表示されていることを確認します。



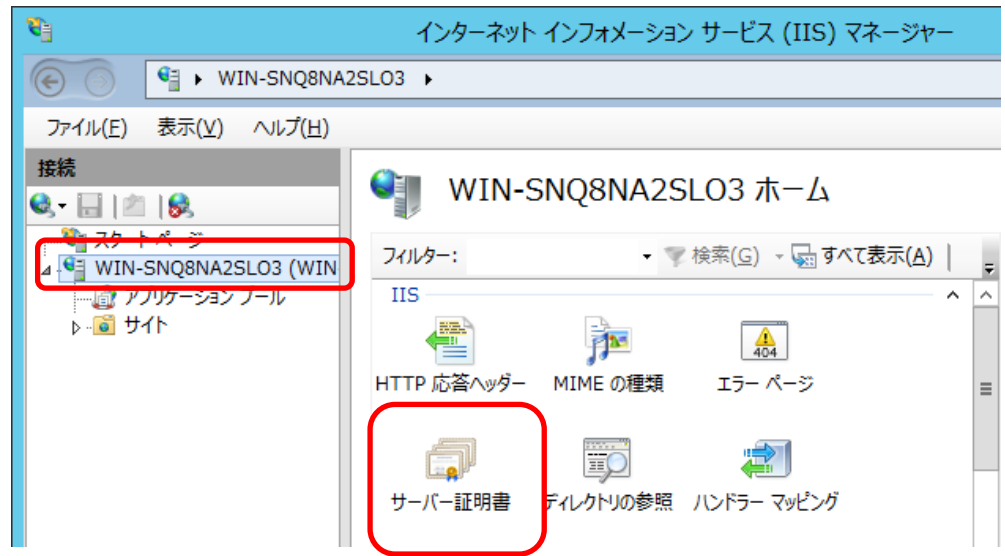
O) 上記画面を閉じる際に、「コンソールの設定をコンソール 1 に保存しますか?」と表示されますので、「いいえ」を選択して終了してください。

以上で中間 CA 証明書のインストールが完了します。

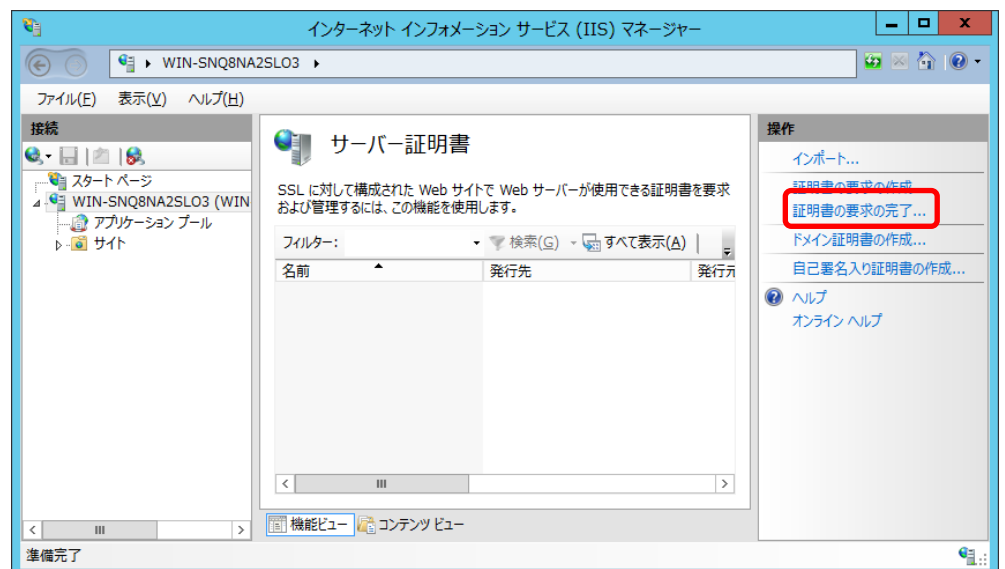
5.2. SSL サーバ証明書のインストール

SSL サーバ証明書のインストールを行います。

- A) 【スタート】メニューから→【インターネット インフォメーション サービス (IIS) マネージャー】を選択して起動し、以下の画面から、【サーバ証明書】をダブルクリックします。



- B) 画面右側の操作メニューから【証明書の要求の完了】をクリックします。



C) 【証明機関の応答が含まれるファイルの名前】に事前にダウンロードしたお客様の SSL サーバ証明書ファイルを指定し、【OK】をクリックします。

※【フレンドリ名】は任意の文字列を入力してください。わかりやすい文字列の入力をおすすめいたします。

※【新しい証明書の証明書ストアを選択してください】は「個人」を選択してください。「Web ホスティング」を選択するとエラーが発生します。

証明書の要求を完了する

証明機関の応答を指定します

証明機関からの応答が含まれるファイルを取得すると、以前に作成した証明書の要求が完了します。

証明機関の応答が含まれるファイルの名前(R):

C:¥201301010004240.cer

フレンドリ名(Y):

Cybertrust Japan

新しい証明書の証明書ストアを選択してください(S):

個人

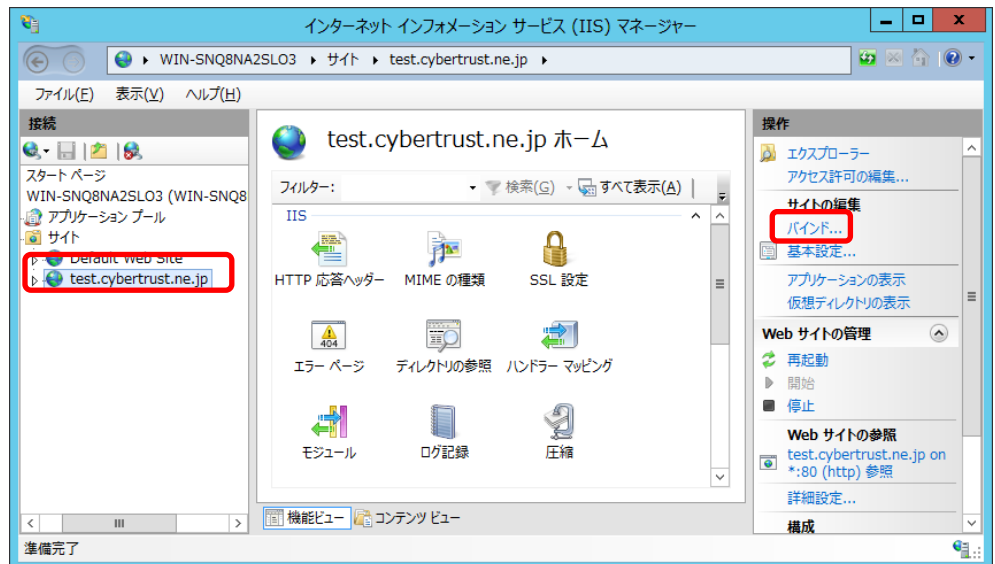
OK キャンセル

以上で SSL サーバ証明書のインストールは完了です。

6. SSL サーバ証明書の適用

インストールした SSL サーバ証明書をご利用の Web サイトへ適用します。

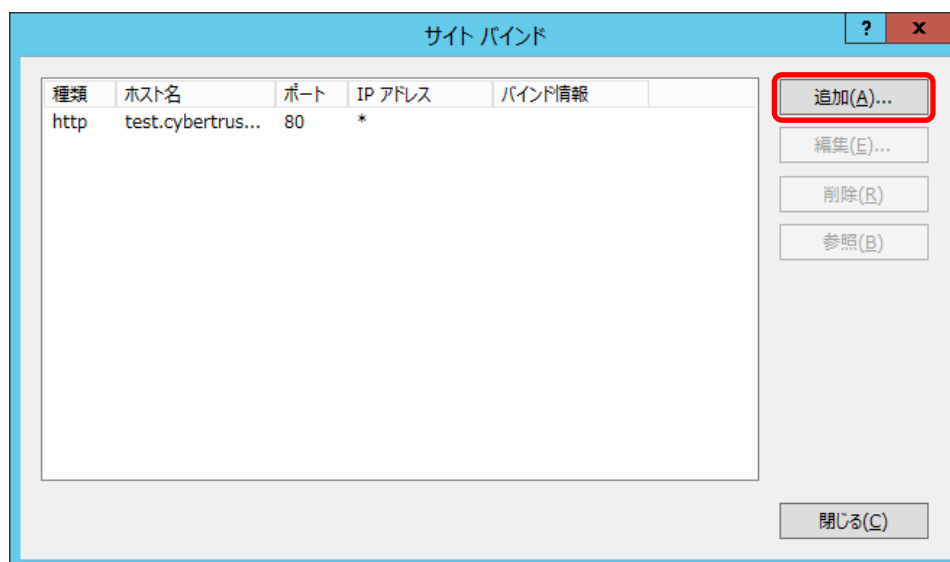
- A) 【インターネット インフォメーション サービス (IIS) マネージャー】画面に戻り、SSL サーバ証明書を適用したい Web サイトを選択し、画面右側の操作メニューから【バインド】をクリックします。



- B) 「サイトバインド」画面が表示されますので、新規の場合は【追加】をクリックします。

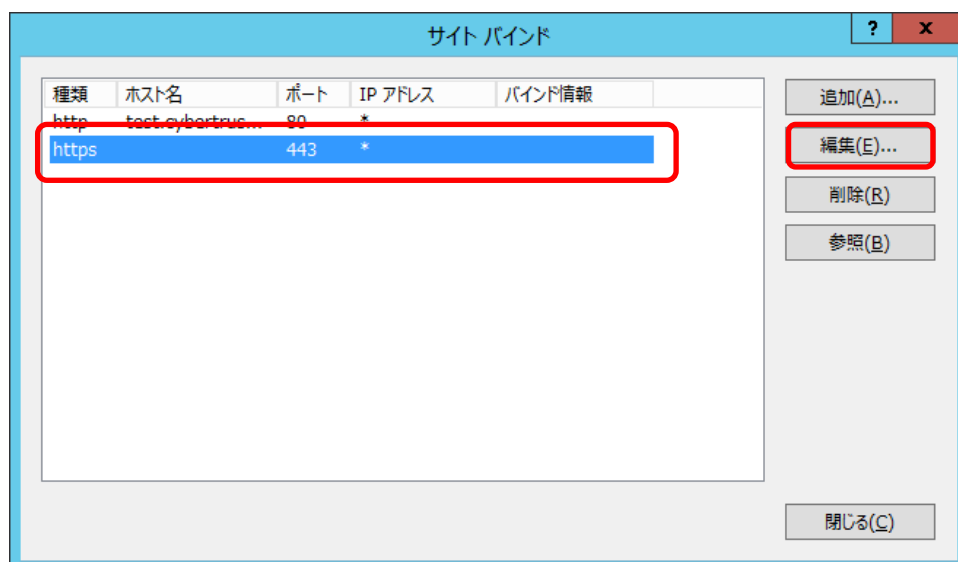
項目	入力内容
種類	https
IP アドレス	サーバ証明書を適用する Web サイトの IP アドレス
ポート	443 (もしくは、任意の SSL ポート番号)
SSL 証明書	インストール時に指定したフレンドリ名や証明書の コモンネームが表示されますので、適用した い SSL サーバ証明書を選択します。

■ 新規の場合



■ 更新の場合

- C) 証明書更新の場合は既に https のバインド設定が存在しますので、そちらを選択して【編集】をクリックします。



D) 【サイトバインドの追加】または【サイトバインドの編集】画面が表示されますので、以下の情報を選択して【OK】をクリックします。

サイトバインドの追加

種類(T): https IP アドレス(I): 未使用の IP アドレスすべて ポート(O): 443

ホスト名(H):

サーバー名表示を要求する(N)

SSL 証明書(E): Cybertrust Japan 選択(L)... 表示(V)...

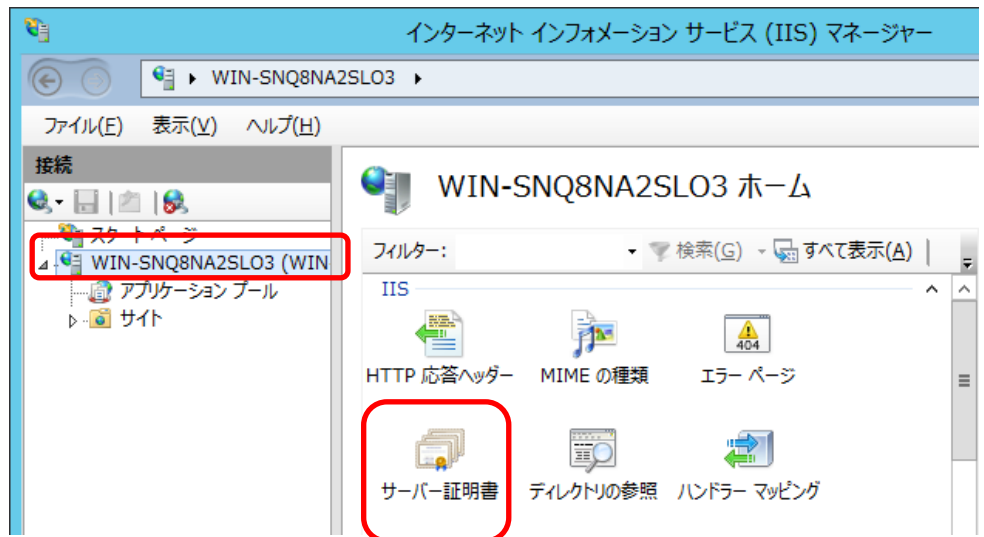
OK キャンセル

以上で SSL サーバ証明書の適用は完了です。

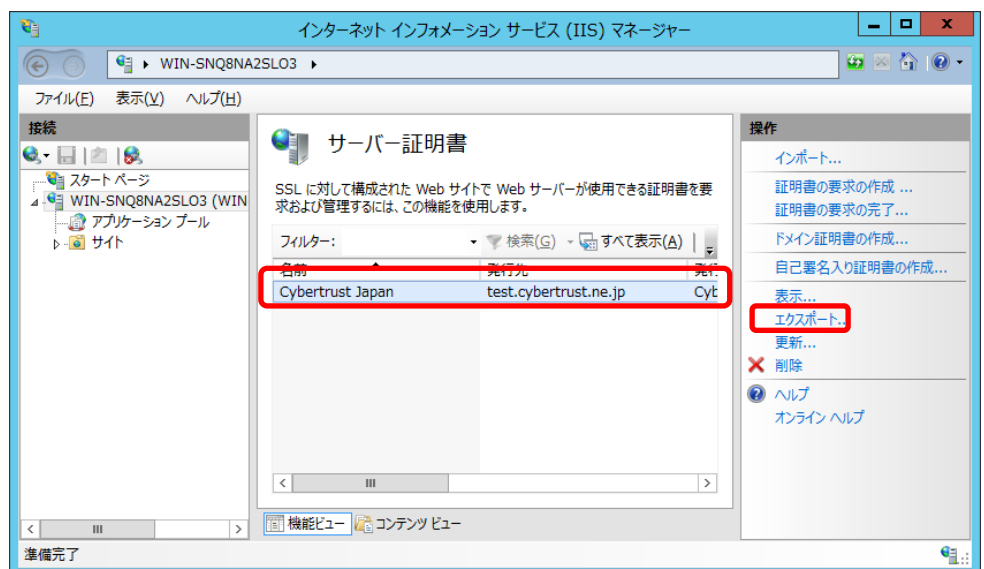
7. 鍵ペアファイルのバックアップ

鍵ペアファイルをバックアップします。

- A) 【スタート】メニューから【インターネット インフォメーション サービス (IIS) マネージャー】を選択して起動します。以下の画面から、【サーバー証明書】をダブルクリックします。

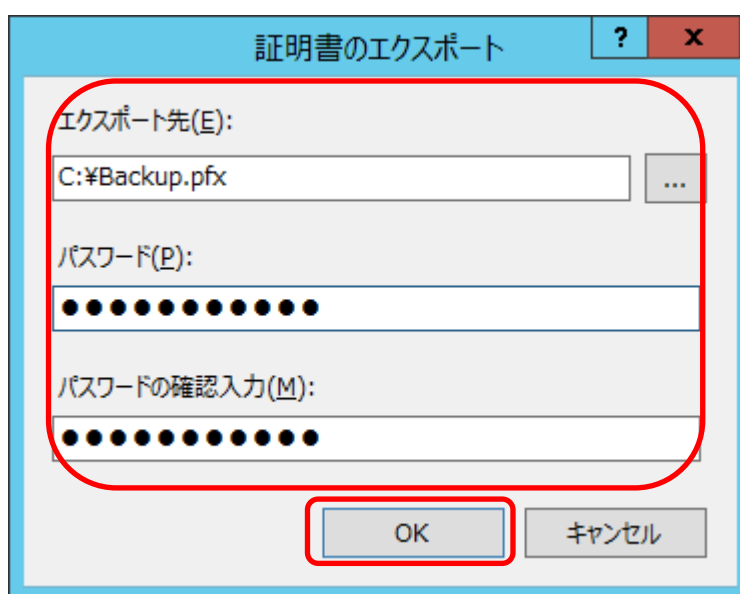


- B) バックアップしたい SSL サーバ証明書を選択し、画面右側の操作メニューから【エクスポート】をクリックします。



C) 【エクスポート先】に保存先のフォルダとファイル名を指定します。ファイルの拡張子は【.pfx】を指定し、【パスワード】、【パスワードの確認入力】に同じパスワードを入力し、【OK】をクリックします。

※指定するパスワードは任意の文字列です。証明書のインポート時に入力が必要となります。



以上で、鍵ペアファイルのバックアップは終了です。

【！】注意事項

- ・ パスワードを紛失した場合には、バックアップに利用できなくなりますので、取り扱いには十分注意してください。
- ・ バックアップファイルは必ず別なメディア(USB や CD 等)にコピーして、安全な場所に保管してください。
- ・ 弊社がお客様の秘密鍵ファイルの情報を受け取ることはございません。あらかじめご了承ください。

SSL 通信の確認

8. SSL 通信の確認

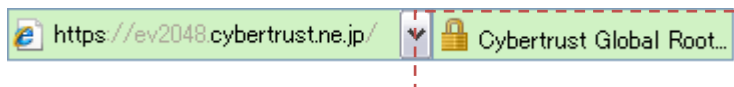
サーバ証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

SSL 通信の確認は設定を行っているサーバ以外の Web ブラウザや携帯電話、スマートフォンなどの携帯端末、「[サーバ証明書の設定確認](#)」から行うことを推奨します。

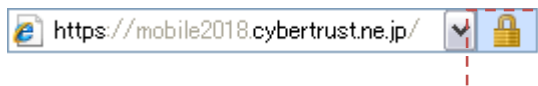
■ 設定確認例

- Internet Explorer 8

<SureServer EV[2048bit]>



<SureServer[2048bit](クロスルート方式を含む)>



- Firefox 12.0

<SureServer EV[2048bit]>



<SureServer[2048bit](クロスルート方式を含む)>



なお、接続時にセキュリティ警告やエラーが表示される場合は、以下よくある質問の「SSL 通信時のセキュリティ警告やエラーについて」をご参照ください。

≫ [SSL 通信時のセキュリティ警告やエラーについて](#)

また、クロスルート設定が正しく反映されない場合は、以下の FAQ をご確認ください。

≫ [\[IIS\] クロスルート設定が正しく反映されません。](#)